Case 1:17-cv-02989-AT Document 865-1 Filed 09/04/20 Page 1 of 9

EXHIBIT A

PLAINTIFF EXHIBIT

29

1:17-cv-02989

Case 1:17-cv-02989-AT Document 865-1 Filed 09/04/20 Page 2 of 9

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, *et al.* *Plaintiffs*, v. BRAD RAFFENSPERGER, *et al.*, *Defendants*.	CIVIL ACTION FILE NO. 1:17-cv-2989-AT

SUPPLEMENTAL DECLARATION OF JACK COBB

Pursuant to 28 U.S.C. § 1746, I, JACK COBB, make the following declaration:

1. My name is Jack Cobb. I am over the age of 21 years, and I am under no legal disability which would prevent me from giving this declaration. If called to testify, I would testify under oath to these facts.

2. I have reviewed the declarations of Dr. Halderman, Mr. Liu, and Mr. Skoglund regarding my prior declaration and offer this additional declaration in response.

Response to Mr. Skoglund

3. Mr. Skoglund claims that the voting system being used by Georgia is not EAC-certified, relying on differences in Engineering Change Order numbers filed with the EAC.

4. Based on these varying numbers, Mr. Skoglund concludes that Democracy Suite 5.5-A (GA) is not EAC-certified, but this is incorrect.

5. ECO 100647 was initially submitted for review in August of 2019. This ECO recommendation to Dominion Voting Systems (DVS) required testing to be performed.

6. Once testing was performed, DVS submitted ECO 100601 for review to the EAC and Pro V&V. This ECO was approved by Pro V&V and recommendation was sent to the EAC for approval (submitted on 4/8/2020 and approved on 4/13/2020).

7. The Georgia designation was added to the D-Suite 5.5-A system name to differentiate this system from the D-Suite 5.5-A and to clarify that additional state testing had been completed.

8. ECO 100647 was utilized in the Pro V&V report because there was not an ECO 100601 at that time. The Georgia report was issued to document the Georgia-specific testing on the scanner and the applicable

VVSG requirements. These tasks included Source Code Review, PCA, TDP Review, System Integration, Accuracy Testing, Volume & Stress, and FCA/Regression Testing.

9. This testing was performed to verify that the new scanner (running version 5.5.3.3) could handle the Georgia requirements. The source code review was performed to whitelist the scanner and ensure no other changes were made to the EAC-certified system.

10. Prior to submitting ECO 100601, additional testing was performed on the new scanner and software version. This included Temp/Power Variation and additional functional testing required in the EAC program.

11. ECO 100601 was submitted to the EAC. This ECO was approved and applied to D-Suite 5.5-A. Due to this approval, there are now three different COTS scanners that may be utilized with the D-Suite 5.5-A system without jeopardizing certification, and thus Georgia's system is EAC-certified.

Response to Mr. Liu

12. I have reviewed Mr. Liu's declaration and will not respond to all of his allegations.

13. Regarding QR Code security, Mr. Liu claims in paragraph that malware running on a BMD will have full access to the necessary material to generate a fraudulent QR Code.

14. But for each election, the encryption keys are passed separately to both the BMD and the ICP from the EMS and are election specific.

Response to Dr. Halderman

15. Dr. Halderman is correct in his very precise statement that Pro V&V has not performed penetration or any security testing on Dominion Democracy Suite 5.5-A. But Pro V&V has performed penetration testing and other security testing on other versions of Dominion Democracy Suite systems.

16. Interestingly, Dr. Halderman claims Pro V&V is limited in its security testing based solely on version numbers but then cites a California Report for Dominion Democracy Suite version 5.10 as a basis that there are vulnerabilities in 5.5-A.

17. But the citation does not support his statement. California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019) at 29,

https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf outlines its review of each of the source code review of the Dominion system and found no vulnerabilities:

> **5. Software Review Testing Summary**
>
> The Secretary of State contracted with SLI to conduct the Source Code Review. The Source Code Review took place at SLI between June 2019, and July 2019. The Dominion DS 5.10 voting system includes proprietary software and firmware. The Dominion DS 5.10 voting system code base was tested to the applicable CVSS requirements.
>
> **ADJ source code vulnerability review**
>
> No discrepancies or vulnerabilities were found within the ADJ source code base reviewed, as a result, no findings were written against the code base.
>
> **EMS source code vulnerability review**
>
> No discrepancies or vulnerabilities were found within the EMS source code base reviewed, as a result, no findings were written against the code base.
>
> **ICC source code vulnerability review**

No discrepancies or vulnerabilities were found within the ICC source code base reviewed, as a result, no findings were written against the code base.

ICE source code vulnerability review

No discrepancies or vulnerabilities were found within the ICE source code base reviewed, as a result, no findings were written against the code base.

ICX source code vulnerability review

No discrepancies or vulnerabilities were found within the ICX source code base reviewed, as a result, no findings were written against the code base.

ICP2 source code vulnerability review

No discrepancies or vulnerabilities were found within the ICP2 source code base reviewed, as a result, no findings were written against the code base.

18. The report concludes, finding "The Dominion Democracy Suite 5.10 voting system, in the configuration tested and documented by the Installation and Use Procedures, meets applicable California Voting System Standards and Elections Code requirements." *Id.*

Case 1:17-cv-02989-AT Document 885-1 Filed 09/04/20 Page 8 of 9

19. Dr. Halderman alleges this report uncovered "serious vulnerabilities" but the report does not support that statement.

20. My earlier statements about "digital signing and encrypting" that Dr. Halderman criticizes come directly from "Dominion Voting 2.02 – Democracy Suite System Overview Version 5.5:146 Dated August 30, 2018 Section 2.6.1.1 Electronic Mobile Ballot" which states:

> "QR Barcode encoded voters selection: Machine readable section of Electronic mobile ballot. Electronic mobile ballot can have multiple QR Barcodes depending of data that need to be encoded (number of available contests, candidates and write-ins). Encoded data is encrypted and signed in order to prevent tampering of user selection and eliminate possibility of error during ballot scanning process

21. After reviewing Dr. Halderman's criticism, I was not as specific in my response as a practitioner as Dr. Halderman is as an academic. The correct technical terms would be the QR codes with the selected voter are encoded and authenticated using SHA256.

Case 1:17-cv-02989-AT Document 885-1 Filed 09/04/20 Page 9 of 9

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 4th day of September, 2020.

Jack Cobb

JACK COBB